DIALOG(R)File 352:Derwent WPI

012521416 **Image available**
WPI Acc No: 1999-327522/199927
XRPX Acc No: N99-245628
Method of determining authenticity of communications terminal user or user group
Patent Assignee: SWISSCOM AG (SWIS-N); SWISSCOM MOBILE AG (SWIS-N)
Inventor: RITTER R
Number of Countries: 080 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9924938	A1	19990520	WO 97CH424	A	19971107	199927	B
AU 9747696	A	19990531	AU 9747696	A	19971107	199941	
			WO 97CH424	A	19971107		
EP 950229	A1	19991020	EP 97910188	A	19971107	199948	
			WO 97CH424	A	19971107		
NO 9904281	A	20000317	WO 97CH424	A	19971107	200025	
			NO 994281	A	19990903		
CN 1249048	A	20000329	CN 97182085	A	19971107	200033	
			WO 97CH424	A	19971107		
BR 9714648	A	20000523	BR 9714648	A	19971107	200035	
			WO 97CH424	A	19971107		
EP 950229	B1	20010124	EP 97910188	A	19971107	200107	
			WO 97CH424	A	19971107		
DE 59702968	G	20010301	DE 502968	A	19971107	200113	
			EP 97910188	A	19971107		
			WO 97CH424	A	19971107		
ES 2154034	T3	20010316	EP 97910188	A	19971107	200126	N
JP 2002511968	W	20020416	WO 97CH424	A	19971107	200242	
			JP 99515987	A	19971107		
US 6657538	B1	20031202	WO 97CH424	A	19971107	200379	
			US 99402054	A	19990928		
RU 2216114	C2	20031110	WO 97CH424	A	19971107	200404	
			RU 99119888	A	19971107		

Priority Applications (No Type Date): WO 97CH424 A 19971107
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9924938	A1	G	230	G07C-009/00	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT
UA UG US UZ VN YU ZW
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9747696	A	Based on patent WO 9924938
EP 950229	A1 G	Based on patent WO 9924938

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

NO 9904281	A	G07C-009/00	
CN 1249048	A	G07C-009/00	
BR 9714648	A	G07C-009/00	Based on patent WO 9924938
EP 950229	B1 G	G07C-009/00	Based on patent WO 9924938

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DE 59702968	G	G07C-009/00	Based on patent EP 950229 Based on patent WO 9924938
ES 2154034	T3	G07C-009/00	Based on patent EP 950229
JP 2002511968	W	22 G06F-015/00	Based on patent WO 9924938
US 6657538	B1	G05B-019/00	Based on patent WO 9924938
RU 2216114	C2	H04M-001/675	Based on patent WO 9924938

Abstract (Basic): WO 9924938 A1

NOVELTY - the method involves acquiring and temporarily storing video information of physical characteristics of a user or group of users at a Point Of Presence, processing the information to extract certain characteristics as a biometric key and storing the key in a table of a biometric server (10) and in a user SIM card (3) whereby at least one biometric key in a table is associated with a corresp. user. The user inserts the SIM card in a communications terminal. Actual physical information are acquired by a local camera and stored and a biometric key is extracted and compared with the stored key to determine authenticity

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for devices, a SIM card and a system for determining people's authenticity

USE - For determining authenticity of communications terminal user or user group

ADVANTAGE - A new and improved method and system are achieved

DESCRIPTION OF DRAWING(S) - the drawing shows a schematic view of the associated arrangement

mobile telephone (1)
biometric server (10)
SIM server (12)
SIM card (3)
pp; 230 DwgNo 1/1

Title Terms: METHOD; DETERMINE; AUTHENTICITY; COMMUNICATE; TERMINAL; USER; USER; GROUP
Derwent Class: S05; T01; T04; T05
International Patent Class (Main): G05B-019/00; G06F-015/00; G07C-009/00; H04M-001/675
International Patent Class (Additional): H04M-001/675
File Segment: EPI

CR21231 ③

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G07C 9/00 — A1

(11) Internationale Veröffentlichungsnummer: **WO 99/24938**

(43) Internationales Veröffentlichungsdatum: 20. Mai 1999 (20.05.99)

(21) Internationales Aktenzeichen: PCT/CH97/00424

(22) Internationales Anmeldedatum: 7. November 1997 (07.11.97)

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SWISSCOM AG [CH/CH]; Viktoriastrasse 21, CH–3030 Bern (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: RITTER, Rudolf [CH/CH]; Rossweidweg 8, CH–3052 Zollikofen (CH).

(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH–3000 Bern 25 (CH).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

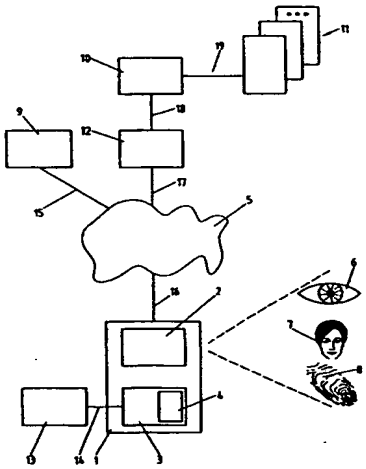
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD, SYSTEM AND DEVICES FOR AUTHENTICATING PERSONS

(54) Bezeichnung: VERFAHREN, SYSTEM UND VORRICHTUNGEN ZUR BESTIMMUNG DER AUTHENTIZITÄT VON PERSONEN

(57) Abstract

The invention concerns a method, system and devices for authenticating a user or group of users of a telecommunication transmitting apparatus (1), which consists in collecting the user's biometric codes, updated in a point of presence (9) and stored in a biometric server (10) as well as on personal SIM cards (3). The authentication is carried out by comparing current biometric codes with the biometric codes stored on the SIM cards (3) by means of trusted third parties (TTP), the current biometric codes being retrieved from current video data transmitted by an integrated video detector (2) to a telecommunication transmitting apparatus (1) or an apparatus external thereto. Depending on the outcome of the authentication, the use of the telecommunication transmitting apparatus (1) can be authorised or prohibited, or the result can be transmitted to an external protected device (13) or still to an intermediate service supplier who, in turn, can respectively grant or deny access to the device (13) and to the services.



(57) Zusammenfassung

Verfahren, System und Vorrichtungen zur Bestimmung der Authentizität eines Benutzers oder einer Benutzergruppe eines Kommunikationsendgerätes (1), wobei biometrische Schlüssel der Benutzer in einem Point of Presence (9) aufgenommen, aktualisiert und in einem biometrischen Server (10) sowie auf persönlichen SIM Karten (3) abgespeichert werden. Die Authentifizierung erfolgt durch den Vergleich von aktuellen biometrischen Schlüsseln mit den auf der SIM Karte (3) gespeicherten biometrischen Schlüsseln unter Zuhilfenahme von Trusted Third Party (TTP) Diensten, wobei die aktuellen biometrischen Schlüssel aus aktuellen Video–Informationen herausgearbeitet werden, welche von einem im Kommunikationsendgerät (1) integrierten (2) oder von einem externen Video–Sensor geliefert werden. Entsprechend dem Resultat der Authentifizierung kann die Benutzung des Kommunikationsendgerätes (1) freigegeben oder verwehrt werden oder das Resultat kann an eine externe gesicherte Vorrichtung (13) oder einen Dienstanbieter übermittelt werden, welche ihrerseits den Zugang zur Vorrichtung (13), respektive den Zugriff auf Dienste, freigeben oder verwehren können.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren, System und Vorrichtungen zur Bestimmung der Authentizität von Personen

Die vorliegende Erfindung betrifft ein Verfahren, ein System und Vorrichtungen zur Bestimmung der Authentizität eines Benutzers oder einer Benutzergruppe eines Kommunikationsendgerätes.

Neben herkömmlichen Methoden um Personen mittels Fotografien und persönlichen Ausweispapieren zu authentifizieren sind im Stand der Technik auch Verfahren bekannt um Personen mittels biometrischen Merkmalen zu authentifizieren. In diesen Verfahren werden mess- und aufnehmbare Körpermerkmale als biometrische Schlüssel registriert und zum Zeitpunkt der Authentifizierung mit den entsprechenden Körpermerkmalen einer zu authentifizierenden Person verglichen. Bekannte Beispiele solcher biometrischen Merkmale umfassen Fingerabdrücke, Augenmuster, Gesichtskonturen oder Charakteristiken der Sprechstimme.

Es ist auch bekannt, dass ein Personal Computer (PC) mit Mitteln, unter anderem einer externen Videokamera, ausgerüstet werden kann, die es dem PC erlauben das Gesicht, respektive einige Gesichtsmerkmale, eines Benutzers in einem Lernprozess aufzunehmen und zu einem späteren Zeitpunkt zu Authentifizierungszwecken wieder zu verwenden, wobei der PC dem Benutzer den Zugang auf den PC nur gestattet wenn er die Gesichtsmerkmale wiedererkennt.

Die Kombination von Video Sensoren mit Kommunikationsendgeräten ist im Zusammenhang mit der Videotelefonie bekannt, die es auch in mobiler Ausführung gibt, in welcher ein Mobilfunktelefon mit einer Videokamera verbunden ist.

Ein Verfahren, das biometrisch messbare Daten wie Augenabdruck oder Fingerabdruck über Kommunikationsnetze, unter anderem mittels Mobiltelefon, als Suchbegriffe zum Auffinden von gespeicherten medizinischen Daten überträgt, ist in DE 39 43 097 A1 beschrieben. In diesem Verfahren wird im wesentlichen ein Individuum mittels biometrischen Merkmalen identifiziert,

so dass auf seine medizinischen Daten zugegriffen werden kann. Es geht dabei aber nicht darum die Authentizität dieses Individuums zu überprüfen oder die Authentizität und Nichtabstreitbarkeit des Ursprungs der in diesem Verfahren über das Kommunikationsnetz ausgetauschten Daten zu gewährleisten.

Es ist die Aufgabe dieser Erfindung ein neues und verbessertes Verfahren und System zur Bestimmung der Authentizität eines Benutzers oder einer Benutzergruppe eines Kommunikationsendgerätes vorzuschlagen.

Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Elemente des kennzeichnenden Teils der unabhängigen Ansprüche 1, 24 und 34 erreicht. Dieses Ziel wird zudem auch durch das System gemäss dem unabhängigen Anspruch 48 erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch die Erfindung dadurch erreicht, dass Körpermerkmale als biometrische Schlüssel gesichert auf einer persönlichen SIM Karte abgespeichert werden und dass diese SIM Karte durch einen Benutzer in ein Kommunikationsgerät eingeführt wird, welches vom Benutzer aktuelle Körpermerkmale und daraus aktuelle biometrische Schlüssel bestimmt und diese zur Authentifizierung des Benutzers mit den abgespeicherten biometrischen Schlüsseln auf der SIM Karte vergleicht. Dies hat den Vorteil, dass eine persönliche Karte den Benutzer in verschiedenen Kommunikationsendgeräten authentifizieren kann, ohne dass der Benutzer Passwörter, welche oft vergessen werden oder auch unrechtmässig eingegeben werden können, verwenden muss und ohne dass ein Benutzer, der die SIM Karte missbräuchlich, zum Beispiel durch Diebstahl oder zufälligen Fund, erworben hat authentifiziert wird. Ein zusätzlicher Vorteil besteht auch darin, dass die SIM Karte auch für eine Benutzergruppe vorbereitet werden kann, indem darauf biometrische Schlüssel für alle der Gruppe angehörenden Benutzer abgespeichert werden.

Um einer missbräuchlichen Authentifizierung, zum Beispiel durch fotografische Imitation von Körpermerkmalen, vorzubeugen werden in den biometrischen Schlüsseln auch Körperbewegungen miteinbezogen.

Erfindungsgemäss kann die Authentifizierung des Benutzers durch das Kommunikationsendgerät dazu dienen einem Benutzer die Benutzung des Kommunikationsendgerätes entsprechend dem Resultat der Authentifizierung zu gestatten oder zu verwehren. Das Resultat der Authentifizierung kann erfindungsgemäss aber auch drahtlos, insbesondere durch ein mobiles Kommunikationsendgerät, an eine externe gesicherte Vorrichtung übermittelt werden, so dass diese externe gesicherte Vorrichtung ihrerseits dem Benutzer entsprechend dem Resultat der Authentifizierung den Zugang zu ihren Diensten oder Gebäulichkeiten gestatten oder verwehren kann.

Erfindungsgemäss wird die Erstaufnahme von biometrischen Schlüsseln in einem mit einem Kommunikationsnetzwerk verbundenen Point of Presence (POP) durchgeführt. Von dort werden sie gesichert über das Kommunikationsnetzwerk an einen biometrischen Server übertragen, wo sie in Tabellen abgespeichert werden, wobei mindestens ein biometrischer Schlüssel in einer Tabelle einem entsprechenden Benutzer zugeordnet wird. Ergänzungen und Aktualisierungen von biometrischen Schlüsseln können ebenso im POP durchgeführt werden. Zudem ist es möglich mit der vorliegenden Erfindung biometrische Schlüssel direkt vom Kommunikationsendgerät aus zu aktualisieren, falls für den betreffenden Benutzer beim biometrischen Server bereits eine Pluralität von biometrischen Schlüsseln bekannt ist.

In der vorliegenden Erfindung werden bei der Authentifizierung und der Übermittlung von biometrischen Schlüsseln vorzugsweise Sicherheitsdienste, zum Beispiel Trusted Third Party (TTP) Dienste, zu Hilfe genommen um die Vertraulichkeit, die Authentizität, die Nichtabstreitbarkeit des Ursprungs und die Integrität von den dabei über ein Kommunikationsnetzwerk ausgetauschten Daten sowie die Authentizität des Senders dieser dabei ausgetauschten Daten zu gewährleisten.

Nachfolgend wird eine Ausführung der vorliegenden Erfindung anhand eines Beispieles beschrieben. Das Beispiel der Ausführung wird durch folgende beigelegte Figur illustriert:

Figur 1 zeigt ein Übersichtsdiagramm mit einem Kommunikationsnetzwerk und einem damit verbundenen mobilen Kommunikationsendgerät mit einer SIM Karte und einem Video Sensor, einen biometrischen Server mit verbundenen Tabellen und SIM Server, einen Point of Presence, sowie eine gesicherte Vorrichtung.

Die Referenznummer 9 bezieht sich auf einen Point of Presence (POP), der beispielsweise mit einem Point of Sale eines Netzwerkbetreibers oder eines Dienstleistungsunternehmens verbunden ist. Der Point of Presence 9 verfügt über mindestens einen Computer der beispielsweise auch als Kommunikationsendgerät dient, vorzugsweise einen Personal Computer oder eine Workstation die an ein Kommunikationsnetzwerk 5, beispielsweise ein Fixnetz 15, angeschlossen sind. Der Point of Presence 9 verfügt zudem über nicht dargestellte, mit dem Computer verbundene Peripherie Geräte zum Aufnehmen von Körpermerkmalen, zum Beispiel eine Video Kamera, die über ein Kabel und eine Video Interface Karte mit dem Computer verbunden ist. Der Computer ist mit einem Programm ausgestattet, welches auf die Peripherie Geräte zugreifen, diese steuern und insbesondere deren aufgenommene Daten lesen, zwischenspeichern und verarbeiten kann. Das Programm verfügt auch über eine Benutzeroberfläche mittels welcher es, beispielsweise durch einen Operator, der ein Angestellter des POP 9 ist, bedient werden kann. Die Benutzeroberfläche hilft dem Operator die Körpermerkmale eines Kunden, zum Beispiel seine Gesichtszüge 7, Augenmuster 6 oder Fingerabrücke 8, aufzunehemen indem es dem Fachmann bekannte Elemente aufweist um beispielsweise die Video Kamera zu justieren, Kontraste einzustellen, Bildausschnitte geeignet darzustellen und dem Operator auch anzuzeigen, wenn die durch das Programm herausgearbeiteten biometrischen Schlüssel fertiggestellt sind, nachdem sie das Programm mit Hilfe des Kunden vor Ort für Authentifizierungszwecke überprüft hat.

Insbesondere für die Aufnahme von Körperbewegungen ist es notwendig, dass das Programm über die Benutzeroberfläche den Kunden und den Operator instruiert zum Beispiel gewisse bestimmte Bewegungen wie beispielsweise Mund oder Augenbewegungen auszuführen. Es ist hier wichtig zu erwähnen, dass in einer Variante die Benutzeroberfläche so ausgeführt werden kann, dass sie für die Aufnahme der biometrischen Schlüssel völlig automatisiert ist und keinen Operator braucht sondern Instruktionen direkt an den Kunden gibt. In dieser Variante sind der Computer mit seinem Bildschirm und der Kamera beispielsweise ähnlich angeordnet wie man dies zum Beispiel von Passfotoautomaten oder Bankautomaten her kennt.

Neben visuellen biometrischen Schlüsseln können in entsprechender Weise und mittels Peripherie Geräten wie Mikrofon und Audio Interface Karte auch Stimmerkmale aufgenommen und als biometrische Schlüssel abgespeichert werden.

Die aufgenommen und erarbeiteten biometrischen Schlüssel eines Kunden können in einem entsprechenden persönlichen Benutzerprofil abgelegt werden sie können aber auch einer Benutzergruppe zugeordnet werden. Das Programm und seine Benutzeroberfläche verfügen über die für einen Fachmann leicht implementierbaren entsprechenden Komponenten, um die dazugehörenden Personaldaten aufzunehemen und in entsprechenden Benutzer- und/oder Benutzergruppenprofile abzulegen. Dabei können zudem auch weitere Sicherheitsinformationen, wie zum Beispiel Sicherheitsstufen um beispielsweise gesicherte Vorrichtungen 13 in verschiedene Stufen von Zugangsrechten auf verschiedene Dienste zu unterteilen, zum Beispiel könnten die Zugriffsrechte eines Benutzer darauf beschränkt werden Gespräche über das Mobilfunktelefon 1 zu führen während ein anderer Benutzer zusätzlich auch andere Funktionen, wie beispielsweise anwählen und ausführen von speziellen Diensten über das Mobilfunktelefon 1, ausführen darf. Andere Beispiele für weitere Sicherheitsinformationen, die eingegeben und abgelegt werden können, sind Angaben zur Gültigkeitsdauer, um beispielsweise die Gültigkeit gewisser Rechte auf eine bestimmte Zeitdauer oder einen bestimmten Zeitpunkt zu begrenzen, Ortsangaben, um beispielsweise

Zugriffsrechte auf Vorrichtungen oder Dienste auf bestimmte geographische Gebiete zu begrenzen, oder persönliche Passworte.

Es ist wichtig, dass die Zuordnung der biometrischen Schlüssel an ein Benutzer- oder Benutzergruppenprofil kontrolliert, zum Beispiel nur durch einen Operator, und unter strikten Authentifizierungsbedingungen, zum Beispiel mittels mehreren offiziellen Ausweispapieren mit Fotografien und eventuell mit bestätigendem Zeugnis von anwesenden Drittpersonen, vorgenommen wird um eine missbräuchliche Zuordnung zu verhindern.

Zum Abschluss der Aufnahme der biometrischen Schlüssel werden die Benutzer- oder Benutzergruppenprofile mit den biometrischen Schlüsseln und Sicherheitsinformationen durch das Programm des Computers gesichert über ein Kommunikationsnetzwerk 5 an einen Server zur Verwaltung der biometrischen Schlüssel, im folgenden ein biometrischer Server 10 genannt, übermittelt und dort in Tabellen 11, die mit dem biometrischen Server 10 verbunden 19 sind, für den entsprechenden Benutzer oder die entsprechende Benutzergruppe abgespeichert. Für den Fachmann ist es klar, dass es verschiedene Möglichkeiten gibt den biometrischen Server 10 mit den Tabellen 11 zu implementieren, zum Beispiel können die Tabellen 11 in einem Datenbank Server sein, welcher sich zusammen mit dem biometrischen Server auf einem Computer befindet oder welcher sich auf einem anderen Computer befindet der mit dem Computer des biometrischen Servers 10 über ein Kommunikationsnetzwerk verbunden ist. Auch für die Abspeicherung der Informationen in den Tabellen 11 gibt es für den Fachmann verschiedene Varianten, auf die hier nicht näher eingegangen wird. Dieselben Informationen werden ebenfalls auf der persönlichen SIM Karte 3 des Benutzers, vorzugsweise eine GSM Karte, oder auf möglicherweise mehreren SIM Karten 3 einer Benutzergruppe in entsprechenden Tabellen 4 abgespeichert, indem sie vom POP 9 an einen SIM Server 12 und von dort, gemäss dem in EP 0689 368 B1 beschriebenen SICAP Verfahren, mittels speziellen Kurzmeldungen über ein Mobilfunknetz, beispielsweise gemäss dem GSM Standard, an die SIM Karte übertragen und dort abgespeichert werden. In einer anderen Variante wird die SIM Karte 3 in ein entsprechendes, nicht dargestelltes Interface des entsprechenden Computers im POP 9 eingeführt und das

Programm speichert die Informationen gesichert in der Tabelle 4 ab. Die somit persönlichen SIM Karten 3 können danach an ihren Benutzer oder an ihre Benutzergruppe übergeben werden.

Für die gesicherte Übermittlung und Abspeicherung von biometrischen Schlüsseln werden vorzugsweise Sicherheitsdienste, zum Beispiel Trusted Third Party (TTP) Dienste, zu Hilfe genommen, um die Vertraulichkeit, die Authentizität, die Nichtabstreitbarkeit des Ursprungs und die Integrität von den übermittelten Daten sowie die Authentizität des Senders dieser übermittelten Daten zu gewährleisten. Es ist durchaus auch möglich die Verschlüsselung mittels einem Point-To-Point Verfahren durchzuführen.

Im POP 9 ist es zudem auch mögliche weitere Dienste, insbesondere Dienste zur Aktualisierung von biometrischen Schlüsseln, zum Beispiel wegen altersbedingten Veränderungen, oder Dienste zur Ergänzungen von weiteren biometrischen Schlüsseln oder anderen Sicherheitsinformationen anzubieten, welche durch den Fachmann entsprechend den obenstehenden Ausführungen implementiert werden können.

Der Benutzer kann seine persönliche SIM Karte 3 in ein Kommunikationsendgerät 1 einschieben und das Gerät einschalten. In diesem Beispiel ist das Kommunikationsendgerät 1 ein Mobilfunktelefon 1, welches mit einem Video-Sensor 2 zur Aufnahme von Körpermerkmalen, wie zum Beispiel Augenmuster 6, Gesichtsmerkmale 7 oder Fingerabdrücke 8, ausgerüstet ist. Der Video-Sensor 2 kann direkt in das Mobilfunktelefon 1 eingebaut sein oder er kann mittels einem Adapter, der beispielsweise selber ein Interface zur Aufnahme einer SIM Karte 3 umfasst, beispielsweise in das Interface für die SIM Karte 3 im Mobilfunktelefon 1 eingeschoben werden. Nach dem Einschalten wird ein Authentifizierungsprogramm, welches sich beispielsweise auf der SIM Karte 3 befindet, aufgestartet und der Benutzer wird beispielsweise mittels des nicht dargestellten Displays des Mobilfunktelefons 1 aufgefordert in den Video-Sensor 2 zu schauen, einen bestimmten Finger auf den Video-Sensor 2 zu halten und/oder in das Mobilfunktelefon 1 zu sprechen. Die Daten welche mittels des Video Sensors 2, und gegebenenfalls mittels des nicht dargestellten Mikrofons des Mobilfunktelefons 1, aufgenommen werden,

werden durch das Authentifizierungsprogramm zwischengespeichert; daraus werden aktuelle biometrische Schlüssel herausgearbeitet, welche zwischengespeichert und mit den abgespeicherten biometrischen Schlüsseln 4 verglichen werden. Zusätzlich zu diesem direkten Vergleich kann die Authentizität und die Integrität der abgespeicherten biometrischen Schlüssel 4 zum Beispiel mit Hilfe von TTP Diensten vom biometrischen Server 10 bestätigt werden. Falls der Vergleich des aktuellen biometrischen Schlüssels mit dem auf der SIM Karte 1 abgespeicherten biometrischen Schlüssel 4 positiv ausfällt und die abgespeicherten biometrischen Schlüssel 4 vom biometrischen Server 10 positiv authentifiziert werden, kann zum Beispiel die weitere Benutzung des Mobilfunktelefons 1 freigegeben werden. Ansonsten kann die weitere Benutzung des Mobilfunktelefons 1 durch diesen Benutzer verwehrt und das Mobilfunktelefon 1 beispielsweise abgeschaltet werden. Die Freigabe kann aufrechterhalten werden bis das Mobilfunktelefon 1 wieder ausgeschaltet wird oder sie kann auch zeitbeschränkt sein, indem der Benutzer nach einer vordefinierten Periode wieder authentifiziert werden muss, dies kann beispielsweise auch automatisch, während der Benutzung des Mobilfunktelefons 1 ausgeführt werden.

Die SIM Karte 3 kommuniziert mit dem biometrischen Server 10 vorzugsweise mittels speziellen Kurzmeldungen, welche über ein Mobilfunknetz 16, beispielsweise gemäss dem GSM Standard, innerhalb des Kommunikationsnetzwerkes 5, an einen SIM Server 12 geschickt werden, welcher ans Kommunikationsnetzwerk 5 über die Verbindung 17 angeschlossen ist und diese speziellen Kurzmeldungen gemäss dem in EP 0689 368 B1 beschriebenen SICAP Verfahren an den biometrischen Server 10 zur Bearbeitung über die Verbindung 18 weiterleitet.

Falls beim biometrischen Server 10 vom Benutzer eine Pluralität von biometrischen Schlüsseln 11 bekannt ist, ist es möglich biometrische Schlüssel 11, die sich zum Beispiel altersbedingt verändert haben, direkt vom Mobilfunktelefon 1 aus zu aktualisieren. Voraussetzung dafür ist, dass der Benutzer durch mindestens einen zweiten nicht veränderungsbedürftigen biometrischen Schlüssel authentifiziert wurde und dass die Qualität der Video-Informationen, welche für die Aktualisierung eines ersten biometrischen

Schlüssels verwendet werden sollen vordefinierten minimalen Anforderungen genügen, dies können zum Beispiel Anforderungen an minimale Lichtverhältnisse oder Bildkontraste oder auch Anforderungen an die maximale Abweichung der neuen biometrischen Schlüssel von den alten biometrischen Schlüsseln sein.

In einer Variante dient die Authentifizierung nicht in erster Linie der Kontrolle der Benutzung des Mobilfunktelefons 1, sondern das Resultat der Authentifizierung, gemäss der obenstehenden Ausführung, wird gesichert und drahtlos an eine externe gesicherte Vorrichtung 13 übermittelt, welche dann ihrerseits den Zugang zu der Vorrichtung 13 entsprechend freigibt oder verwehrt. Zusammen mit dem Resultat der Authentifizierung können auch Personaldaten des Benutzers an die gesicherte Vorrichtung 13 übertragen werden, so dass die gesicherte Vorrichtung 13 auf Grund dieser Personaldaten des authentifizierten Benutzers den Zugang freigeben oder verweheren kann. In einer anderen Variante werden der gesicherten Vorrichtung 13 zusammen mit dem Resultat der Authentifizierung weitere Sicherheitsinformationenen des Benutzers, wie beispielsweise Sicherheitsstufen, Ortsangaben und Angaben zur Gültigkeitsdauer, übermittelt, womit die gesicherte Vorrichtung 13 den Entscheid zur Freigabe oder Verwehrung des Zugangs treffen kann. In einer anderen Variante übermittelt die gesicherte Vorrichtung 13 auf Anfrage Informationen zu ihrer Identifikation an das Mobilfunktelefon 1, womit das Mobilfunktelefon 1 während des Authentifizierungsprozesses mittels weiteren Sicherheitsinformationen des Benutzers, wie beispielsweise Sicherheitsstufen, Ortsangaben und Angaben zur Gültigkeitsdauer, auch Entscheide über den Zugang des Benutzers zu der betreffenden gesicherten Vorrichtung 13 fällen und an die gesicherte Vorrichtung 13 übermitteln kann. Die externe gesicherte Vorrichtung 13 ist zum Beispiel ein Apparat, beispielsweise ein Bank-Automat oder ein Video-Terminal für Informationsabfragen, der Eingang zu einem gesicherten Gebäude, wie beispielsweise eine geheime industrielle Fertigungsanlage, eine Polizeikaserne oder ein Atomkraftwerk, oder der Eingang zu einem gesperrten Gelände, wie beispielsweise eine Armee Basis, ein Flughafen oder ein Fabrikareal. Die drahtlose Übermittlung kann beispielsweise kontaktlos über eine induktive Verbindung 14 mittels einer elektrischen Spule auf der SIM Karte 3 ausgeführt werden. Das

Mobilfunktelefon 1 kann die Übermittlung an die gesicherte Vorrichtung 13 auch mittels einer nicht dargestellten kontaktlosen Infrarot-Schnittstelle oder mittels Kurzmeldungen ausführen. Die Übermittlung erfolgt jeweils gesichert, zum Beispiel unter Zuhilfenahme von TTP Diensten oder mittels einem Point-To-Point Verfahren.

In einer weiteren Variante befindet sich der Video-Sensor ausserhalb des Mobilfunktelefons 1, zum Beispiel in der externen gesicherten Vorrichtung 13. In dieser Variante werden die Video-Informationen durch die externe Video Kamera aufgenommen und zur Auswertung drahtlos auf das Mobilfunktelefon übertragen. Die drahtlose Übertragung kann beispielsweise kontaktlos über eine induktive Verbindung 14 mittels einer elektrischen Spule auf der SIM Karte 3 ausgeführt werden. Die gesicherte Vorrichtung 13 kann die Übermittlung an das Mobilfunktelefon 1 auch mittels einer nicht dargestellten kontaktlosen Infrarot-Schnittstelle oder mittels Kurzmeldungen ausführen. Die Übermittlung erfolgt jeweils gesichert zum Beispiel unter Zuhilfenahme von TTP Diensten oder mittels einem Point-To-Point Verfahren.

Es muss hier auch erwähnt werden, dass neben Mobilfunktelefonen 1 auch andere Kommunikationsendgeräte, wie zum Beispiel Personal Computers, Laptop Computers, oder Palmtop Computers, diese Authentifizierungsverfahren ausführen können wenn sie mit einer SIM Karte 3 und mit Peripherie Geräten zur Aufnahme von Körpermerkmalen ausgerüstet werden. Zudem muss sich die Anwendung der Authentifizierung nicht auf die Zugangskontrolle für Kommunikationsendgeräte oder externe gesicherte Vorrichtungen 13 beschränken, sondern sie kann durchaus auch für die Zugriffskontrolle auf Dienste angewendet werden, insbesondere auch auf Dienste die über das Kommunikationsnetzwerk 5 verfügbar sind, welches auch das Internet umfassen kann. In diesen Fällen wird das Resultat der Authentifizierung an den betreffenden Dienstanbieter, beispielsweise einen automatisierten Internet Site, übermittelt welcher demzufolge Dienste freigeben oder verwehren kann. Das Resultat der Authentifizierung wird eventuell zusammen mit Informationen über Zugriffsrechte des Benutzers auf die betreffenden Dienste oder zusammen mit Personaldaten des Benutzers an den

Dienstanbieter übermittelt, wie dies obenstehend im Zusammenhang mit gesicherten Vorrichtungen 13 beschrieben wurde.

Es ist durchaus möglich, dass dieses Verfahren und System durch einen Dienstleistungsanbieter gegen Bezahlung als Dienst an Dritte angeboten werden kann, welche zum Beispiel daran interessiert sind ihre Vorrichtungen, Gebäulichkeiten, Gebiete oder Dienste zu sichern.

Ansprüche

1. Verfahren zur Bestimmung der Authentizität eines Benutzers oder einer Benutzergruppe eines Kommunikationsendgerätes (1), dadurch gekennzeichnet, dass es folgende Schritte umfasst:

- Aufnahme und Zwischenspeicherung von Video-Informationen von Körpermerkmalen (6, 7, 8) des Benutzers oder der Benutzergruppe in einem Point of Presence (POP) (9),

- Verarbeitung der genannten zwischengespeicherten Video-Informationen, so dass bestimmte Merkmale als biometrische Schlüssel herausgearbeitet werden,

- Abspeichern der biometrischen Schlüssel in Tabellen (11) eines biometrischen Servers (10) und in einer SIM Karte (3) des Benutzers oder der Benutzergruppe, wobei mindestens ein biometrischer Schlüssel in einer Tabelle (4, 11) einem entsprechenden Benutzer zugeordnet wird,

- Einführen der SIM Karte (3), die mindestens einen persönlichen biometrischen Schlüssel enthält, in ein Kommunikationsendgerät (1) durch den Benutzer,

- Aufnehmen und Zwischenspeichern von aktuellen Video-Informationen von mindestens einem Körpermerkmal (6, 7, 8) des Benutzers über einen Video-Sensor (2),

- Verarbeitung der zwischengespeicherten aktuellen Video-Informationen des Benutzers, so dass mindestens ein bestimmtes Merkmal als aktueller biometrischer Schlüssel herausgearbeitet und zwischengespeichert wird,

- Bestimmung der Authentizität durch Vergleich des mindestens einen zwischengespeicherten aktuellen biometrischen Schlüssels des Benutzers mit dem mindestens einen gespeicherten biometrischen Schlüssel

(4), wobei bei einem positiven Vergleich die Authentizität als sichergestellt gilt und bei einem negativen Vergleich die Authentizität als nicht sichergestellt gilt.

2. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass beim Aufnehmen und Zwischenspeichern von aktuellen Video-Informationen der Video-Sensor (2) insbesondere auch Bewegung registriert und dies bei der Bestimmung der Authentizität miteinbezogen wird.

3. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Zwischenspeichern von aktuellen Video-Informationen, deren Verarbeitung und erneute Zwischenspeicherung, die Bestimmung der Authentizität durch den Vergleich mit den abgespeicherten biometrischen Schlüsseln (4) durch die SIM Karte (3) ausgeführt wird.

4. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass bei der Übermittlung von mindestens gewissen Meldungen Sicherheitsdienste des TTP (TTP Dienste) zu Hilfe genommen werden um die Vertraulichkeit, die Authentizität, die Nichtabstreitbarkeit des Ursprungs und die Integrität von den dabei über ein Kommunikationsnetzwerk (5) ausgetauschten Daten sowie die Authentizität des Senders dieser dabei ausgetauschten Daten zu gewährleisten.

5. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im POP (9) zusätzlich zu den biometrischen Schlüsseln unter Zuhilfenahme von TTP Diensten Sicherheitsinformationen aufgenommen und in den Tabellen (11) des biometrischen Servers (10) und in der SIM Karte (3) abgespeichert werden, wobei sie in Tabellen (4, 11) den entsprechenden Benutzern oder Benutzergruppen zugeordnet werden und dass diese Sicherheitsinformationen bei der Bestimmung der Authentizität miteinbezogen werden.

6. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die zusätzlichen Sicherheitsinformationen Sicherheitsstufen umfassen.

7. Verfahren gemäss einem der Ansprüche 5 bis 6, dadurch gekennzeichnet, dass die zusätzlichen Sicherheitsinformationen Gültigkeitsdauerangaben umfassen.

8. Verfahren gemäss einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass die zusätzlichen Sicherheitsinformationen Ortsangaben umfassen.

9. Verfahren gemäss einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, dass die zusätzlichen Sicherheitsinformationen Passwörter umfassen.

10. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im POP (9) bereits bestehende Informationen für entsprechende Benutzer oder Benutzergruppen unter Zuhilfenahme von TTP Diensten aktualisiert und ergänzt werden können.

11. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass biometrische Schlüssel, die in den Tabellen (4, 11) des biometrischen Servers (10) und in der SIM Karte (3) eines Kommunikationsendgerätes (1) abgespeichert sind, unter Zuhilfenahme von TTP Diensten direkt vom Kommunikationsendgerät (1) aus aktualisiert werden können.

12. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass inbesondere Gesichtsmerkmale (7) als biometrische Schlüssel herausgearbeitet werden.

13. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass inbesondere Augenmuster (6) als biometrische Schlüssel herausgearbeitet werden.

14. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass inbesondere Fingerabdrücke (8) als biometrische Schlüssel herausgearbeitet werden.

15. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass neben visuellen Merkmalen inbesondere auch Sprechstimmerkmale als biometrische Schlüssel aufgenommen werden.

16. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Aufnehmen von aktuellen Video-Informationen mit einem Video-Sensor (2) ausgeführt wird, der sich im Kommunikationsgerät (1) befindet.

17. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Aufnehmen von aktuellen Video-Informationen mit einem Video-Sensor ausgeführt wird, der sich ausserhalb des Kommunikationsgerätes (1) befindet, wobei die Video-Informationen zur Zwischenspeicherung und Weiterverarbeitung ans Kommunikationsgerät (1) übermittelt werden.

18. Verfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die Übermittlung der aktuellen Video-Informationen ans Kommunikationsgerät (1) induktiv (14) über eine Spule in einer SIM Karte (3) ausgeführt wird.

19. Verfahren gemäss dem vorhergehenden Anspruch 17, dadurch gekennzeichnet, dass die Übermittlung der aktuellen Video-Informationen ans Kommunikationsgerät (1) mittels Infrarot ausgeführt wird.

20. Verfahren gemäss dem vorhergehenden Anspruch 17, dadurch gekennzeichnet, dass die Übermittlung der aktuellen Video-Informationen ans Kommunikationsgerät (1) mittels Kurzmeldungen ausgeführt wird.

21. Verfahren gemäss einem der Ansprüche 17 bis 20, dadurch gekennzeichnet, dass die Video-Informationen unter Zuhilfenahme von TTP Diensten ans Kommunikationsgerät (1) übermittelt werden.

22. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Kommunikation zwischen der SIM Karte (3)

im Kommunikationsendgerät (1) und dem biometrischen Server (10) mittels speziellen Meldungen über einen SIM Server (12) ausgeführt wird.

23. Verfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass für den Fall der Sicherstellung der Authentizität des Benutzers die Benützung des Kommunikationsendgerätes (1) freigegeben werden kann während für den Fall der Nicht-Sicherstellung der Authentizität des Benutzers die Benützung des Kommunikationsendgerätes (1) nicht freigegeben wird.

24. Mobile Vorrichtung (1) für das Telefonieren über Funk, welche ein Interface zum Aufnehmen einer SIM Karte (3) und einen Video-Sensor (2) zur Aufnahme von Video-Informationen umfasst, dadurch gekennzeichnet, dass sie über Speichermittel verfügt um biometrische Schlüssel zu speichern (4), dass sie Verarbeitungsmittel umfasst um aus den genannten Video-Informationen bestimmte Merkmale herauszuarbeiten und dass sie Vergleichsmittel umfasst um diese bestimmten Merkmale mit den gespeicherten biometrischen Schlüsseln (4) zu vergleichen.

25. Vorrichtung (1) gemäss dem vorhergenden Anspruch, dadurch gekennzeichnet, dass sie ein Mobilfunktelefon umfasst in welches der Video-Sensor (2) direkt eingebaut ist.

26. Vorrichtung (1) gemäss dem Anspruch 24, dadurch gekennzeichnet, dass sie einen Adapter umfasst in welchen der Video-Sensor eingebaut ist.

27. Vorrichtung (1) gemäss einem der Ansprüche 24 bis 26, dadurch gekennzeichnet, dass sie eine SIM Karte (3) umfasst, welche sich im genannten Interface zum Aufnehmen der SIM Karte (3) befindet und in welcher die genannten biometrischen Schlüssel (4) gespeichert sind.

28. Vorrichtung (1) gemäss dem vorhergenden Anspruch, dadurch gekennzeichnet, dass die genannten Speichermittel, Verarbeitungsmittel und Vergleichsmittel auf der SIM Karte (3) implementiert sind.

29. Vorrichtung (1) gemäss einem der Ansprüche 24 bis 28, dadurch gekennzeichnet, dass die Verarbeitungsmittel speziell darauf eingerichtet sind aus den Video-Informationen Körpermerkmale (6, 7, 8) von Personen zu ermitteln.

30. Vorrichtung (1) gemäss dem vorhergenden Anspruch, dadurch gekennzeichnet, dass die Körpermerkmale auf welche die Verarbeitungsmittel speziell eingerichtet sind Gesichtszüge (7) umfassen.

31. Vorrichtung (1) gemäss einem der Ansprüche 29 bis 30, dadurch gekennzeichnet, dass die Körpermerkmale auf welche die Verarbeitungsmittel speziell eingerichtet sind Augenmuster (6) umfassen.

32. Vorrichtung (1) gemäss einem der Ansprüche 29 bis 31, dadurch gekennzeichnet, dass die Körpermerkmale auf welche die Verarbeitungsmittel speziell eingerichtet sind Fingerabdrücke (8) umfassen.

33. Vorrichtung (1) gemäss einem der Ansprüche 24 bis 32, dadurch gekennzeichnet, dass der biometrische Schlüssel auch Körperbewegungen umfasst.

34. Subscriber Identity Module (SIM) Karte (3) für ein Kommunikationsendgerät (1) dadurch gekennzeichnet, dass mindestens ein biometrischer Schlüssel zur Bestimmung der Authentizität einer Person oder einer Gruppe von Personen im Speicher (4) der SIM Karte (3) gespeichert ist.

35. SIM Karte (3) gemäss dem vorhergenden Anspruch, dadurch gekennzeichnet, dass der abgespeicherte biometrische Schlüssel Gesichtsmerkmale (7) umfasst.

36. SIM Karte (3) gemäss einem der Ansprüche 34 bis 35, dadurch gekennzeichnet, dass der abgespeicherte biometrische Schlüssel Augenmuster (6) umfasst.

37. SIM Karte (3) gemäss einem der Ansprüche 34 bis 36, dadurch gekennzeichnet, dass der abgespeicherte biometrische Schlüssel Fingerabdrücke (8) umfasst.

38. SIM Karte (3) gemäss einem der Ansprüche 34 bis 37, dadurch gekennzeichnet, dass die abgespeicherten biometrischen Schlüssel (4) neben visuellen Merkmalen auch Sprechstimmerkmale umfassen.

39. SIM Karte (3) gemäss einem der Ansprüche 34 bis 38, dadurch gekennzeichnet, dass andere Sicherheitsinformationen auf der SIM Karte (3) gespeichert sind.

40. SIM Karte (3) gemäss dem vorhergenden Anspruch, dadurch gekennzeichnet, dass die abgespeicherten Sicherheitsinformationen Sicherheitsstufen umfassen.

41. SIM Karte (3) gemäss einem der Ansprüche 39 bis 40, dadurch gekennzeichnet, dass die abgespeicherten Sicherheitsinformationen Gültigkeitsdauerangaben umfassen.

42. SIM Karte (3) gemäss einem der Ansprüche 39 bis 41, dadurch gekennzeichnet, dass die abgespeicherten Sicherheitsinformationen Ortsangaben umfassen.

43. SIM Karte (3) gemäss einem der Ansprüche 39 bis 42, dadurch gekennzeichnet, dass die abgespeicherten Sicherheitsinformationen Passwörter umfassen.

44. SIM Karte (3) gemäss einem der Ansprüche 34 bis 43, dadurch gekennzeichnet, dass sie über Mittel verfügt um Video-Informationen zwischenzuspeichern, um aus den zwischengespeicherten Video-Informationen bestimmte Merkmale herauszuarbeiten und diese bestimmten Merkmale zwischenzuspeichern, um die genannten zwischengespeicherten Merkmale mit den genannten gespeicherten biometrischen Schlüsseln (4) zu vergleichen und

um in Äbhängigkeit des Resultates dieses Vergleichs verschiedene weitere Schritte auszuführen.

45. SIM Karte (3) gemäss einem der Ansprüche 34 bis 44, dadurch gekennzeichnet, dass sie über Mittel verfügt um digital signierte und chiffrierte Meldungen, insbesondere unter Zuhilfenahme von Trusted Third Party (TTP) Diensten, zu verfassen und zu dechiffrieren damit die Vertraulichkeit, die Authentizität, die Nichtabstreitbarkeit des Ursprungs und die Integrität von diesen Meldungen sowie die Authentizität von Sendern dieser Meldungen gewährleistet ist, und um diese Meldungen an einen biometrischen Server (10) zu übertragen.

46. SIM Karte (3) gemäss einem der Ansprüche 34 bis 45, dadurch gekennzeichnet, dass sie über Mittel verfügt um Meldungen insbesondere gemäss einem Point-To-Point Verfahren zu verfassen und zu dechiffrieren.

47. SIM Karte (3) gemäss einem der Ansprüche 34 bis 46, dadurch gekennzeichnet, dass sie eine elektrische Spule umfasst über welche sie induktiv (14) mit externen, gesicherten Vorrichtungen (13) Daten betreffend deren Sicherheit austauschen kann.

48. System zur Ausführung eines Verfahrens gemäss den Ansprüchen 1 bis 23 mit Hilfe von mobilen Vorrichtungen (1) gemäss den Ansprüchen 24 bis 33, die SIM Karten (3) gemäss den Ansprüchen 34 bis 47 umfassen und die als Kommunikationsendgeräte (1) über ein Kommunikationsnetzwerk (5) miteinander verbunden sind.

49. System gemäss dem vorhergehenen Anspruch, dadurch gekennzeichnet, dass das Kommunikationsnetzwerk (5) ein Mobilfunknetz umfasst.

50. System gemäss dem vorhergehenen Anspruch, dadurch gekennzeichnet, dass das Mobilfunknetz ein Mobilfunknetz gemäss dem GSM Standard ist.

51. System gemäss einem der Ansprüche 48 bis 50, dadurch gekennzeichnet, dass das Kommunikationsnetzwerk (5) ein Fixnetz umfasst.

52. System gemäss einem der Ansprüche 48 bis 51, dadurch gekennzeichnet, dass das Kommunikationsnetzwerk (5) das Internet umfasst.

53. System gemäss einem der vorhergehenen Ansprüche 48 bis 52, dadurch gekennzeichnet, dass es weitere Kommunikationsendgeräte, insbesondere Personal Computers, Laptops und Palmtops umfasst, von denen mindestens gewisse mit einem Video-Sensor ausgestattet sind und die über das Kommunikationsnetzwerk (5) miteinander verbunden sind.

54. System gemäss einem der Ansprüche 48 bis 53, dadurch gekennzeichnet, dass es zusätzlich externe gesicherte Vorrichtungen (13) umfasst welche mit Kommunikationsendgeräten (1) drahtlos und unter Zuhilfenahme von TTP Diensten kommunizieren können.

55. System gemäss dem vorhergehenen Anspruch, dadurch gekennzeichnet, dass die gesicherte Vorrichtung (13) mittels Induktion (14) mit der SIM Karte (3) im Kommunikationsendgerät (1) kommuniziert.

56. System gemäss dem vorhergehenen Anspruch 54, dadurch gekennzeichnet, dass die gesicherte Vorrichtung (13) mittels Infrarot mit dem Kommunikationsendgerät (1) kommuniziert.

57. System gemäss dem vorhergehenen Anspruch 54, dadurch gekennzeichnet, dass die gesicherte Vorrichtung (13) mittels Kurzmeldungen mit dem Kommunikationsendgerät (1) kommuniziert.

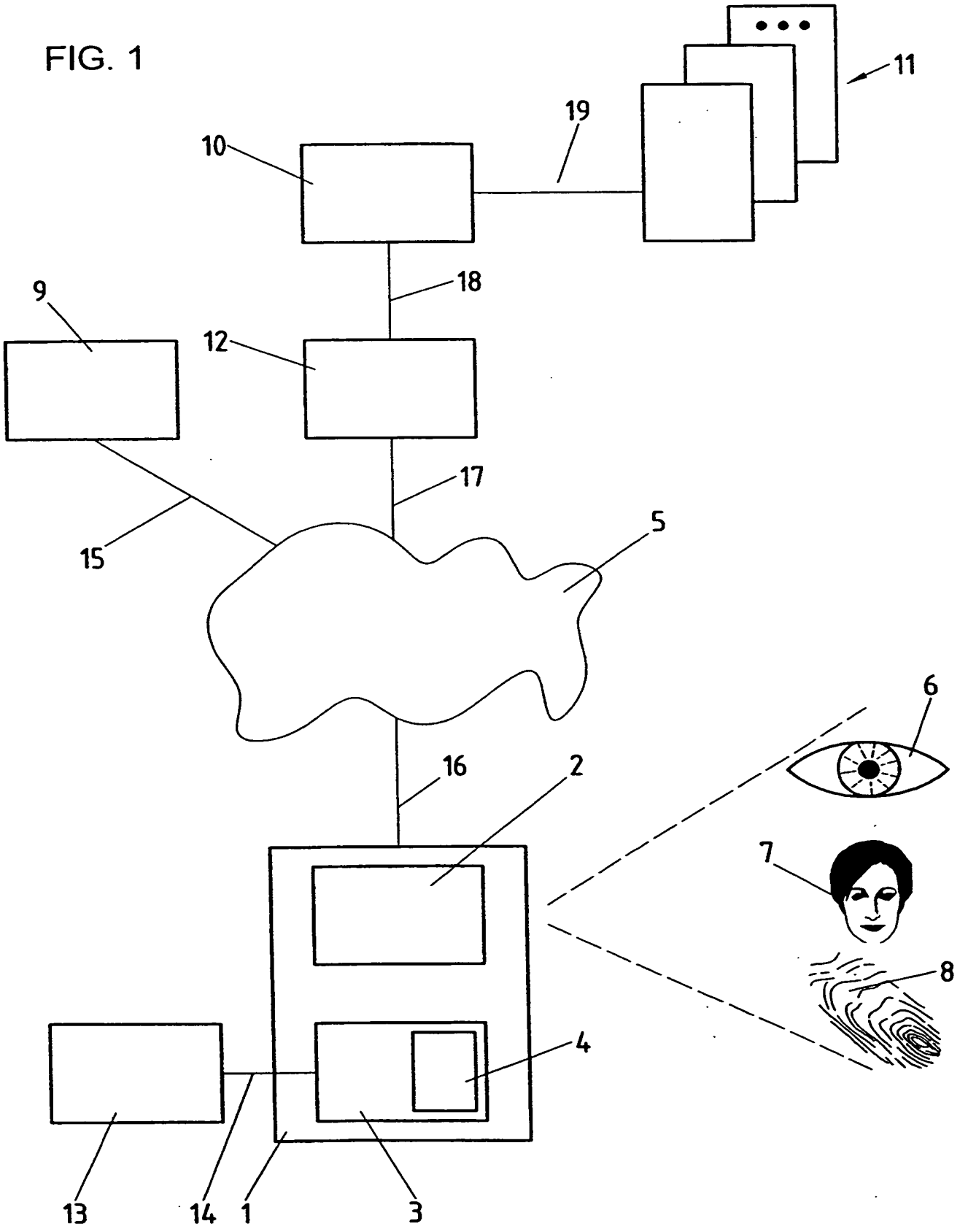
58. System gemäss einem der Ansprüche 48 bis 57, dadurch gekennzeichnet, dass es gesicherte Vorrichtungen (13) umfasst die mit Video Kameras ausgerüstet sind.

59. System gemäss einem der Ansprüche 48 bis 58, dadurch gekennzeichnet, dass es SIM Server (12) umfasst über welche die SIM Karten

(3) in den Kommunikationsgeräten (1) mittels speziellen Meldungen mit einem biometrischen Server (10) kommunizieren.

60. System gemäss einem der Ansprüche 48 bis 59, dadurch gekennzeichnet, dass es biometrischen Server (10) umfasst, welche mit Tabellen (11) verbunden sind in denen biometrische Schlüssel abgespeichert sind, wobei mindestens ein biometrischer Schlüssel in einer Tabelle (11) einem entsprechenden Benutzer zugeordnet ist.

FIG. 1



INTERNATIONAL SEARCH REPORT

Inter. ...nal Application No
PCT/CH 97/00424

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 see claim 1; figure 1	1,24,34, 48
Y	WO 96 18169 A (KRETZSCHMAR LOREN ;DAVIS VICTORIA (US)) 13 June 1996 see claim 1; figure 1	1,24,34, 48
A		2-23, 25-33, 35-47, 49-60

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 July 1998	31/07/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. ...nal Application No
PCT/CH 97/00424

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	PATENT ABSTRACTS OF JAPAN vol. 096, no. 008, 30 August 1996 & JP 08 088841 A (ADO MANIYUARU:KK), 2 April 1996,	1,24,34, 48
A	see abstract	2-23, 25-33, 35-47, 49-60
A	US 5 420 908 A (HODGES STEVEN J ET AL) 30 May 1995 see claim 1; figure 1	1-60
A	US 5 131 038 A (PUHL LARRY C ET AL) 14 July 1992 see claim 1; figure 1	1-60

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CH 97/00424

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
WO 9618169 A	13-06-1996	AU 4894796 A	26-06-1996
US 5420908 A	30-05-1995	CA 2114040 A	12-09-1994
		US 5541977 A	30-07-1996
		US 5754952 A	19-05-1998
US 5131038 A	14-07-1992	NONE	

INTERNATIONALER RECHERCHENBERICHT

Inten. ...nales Aktenzeichen
PCT/CH 97/00424

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
E	WO 98 11750 A (SUBBIAH SUBRAMANIAN ;LI YANG (US); RAO D RAMESK K (US)) 19.März 1998 siehe Anspruch 1; Abbildung 1	1,24,34, 48
Y	WO 96 18169 A (KRETZSCHMAR LOREN ;DAVIS VICTORIA (US)) 13.Juni 1996	1,24,34, 48
A	siehe Anspruch 1; Abbildung 1	2-23, 25-33, 35-47, 49-60

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23.Juli 1998	31/07/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/CH 97/00424

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	PATENT ABSTRACTS OF JAPAN vol. 096, no. 008, 30.August 1996 & JP 08 088841 A (ADO MANIYUARU:KK), 2.April 1996,	1,24,34, 48
A	siehe Zusammenfassung	2-23, 25-33, 35-47, 49-60
A	US 5 420 908 A (HODGES STEVEN J ET AL) 30.Mai 1995 siehe Anspruch 1; Abbildung 1	1-60
A	US 5 131 038 A (PUHL LARRY C ET AL) 14.Juli 1992 siehe Anspruch 1; Abbildung 1	1-60

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/CH 97/00424

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9811750 A	19-03-1998	AU 4341797 A	02-04-1998
WO 9618169 A	13-06-1996	AU 4894796 A	26-06-1996
US 5420908 A	30-05-1995	CA 2114040 A	12-09-1994
		US 5541977 A	30-07-1996
		US 5754952 A	19-05-1998
US 5131038 A	14-07-1992	KEINE	